AMENDMENTS TO THE CLAIMS

The following listing of claims replaces all prior versions of the claims and all prior listings of the claims in the present application.

1. (canceled)

2. (currently amended) A multiple modulus selector of a computer system, communication network, or computer system and communication network that uses a public-key cryptographic algorithm, the multiple modulus selector comprising:

a modulus recoder ~~for receiving~~ adapted to receive an n-bit modulus M, a previous sum, and a current partial product to generate a first selection signal;

a modulus selector ~~for receiving~~ adapted to receive the n-bit modulus M, the previous sum, the current partial product, and a multiplicand to generate a second selection signal; and

a multiplexer ~~for receiving~~ adapted to receive inputs -M, 0, M, and 2M, ~~and selecting~~ adapted to select one of the inputs -M, 0, M, and 2M based on the first selection signal in an integer modular multiplication mode, and ~~selecting~~ adapted to select one of the inputs -M, 0, M, and 2M based on the second selection signal in a polynomial modular multiplication mode.

3. (currently amended) The multiple modulus selector ~~as recited in~~ of claim 2, wherein the input -M is obtained by inverting the modulus M.

4. (currently amended) The multiple modulus selector ~~as recited in~~ of claim 2, wherein the input [[-]]2M is obtained by shifting the modulus M.

5. (currently amended) The multiple modulus selector ~~as recited in~~ of claim 2, wherein the modulus M is stored in a register.

6. (currently amended) The multiple modulus selector ~~as recited in~~ of claim 2, wherein the modulus recoder further generates a multiple modulus negation indicating signal ~~(NEG_MM)~~ that is input to an accumulator.

7. (currently amended) The multiple modulus selector ~~as recited in~~ of claim 2, wherein the n-bit modulus M includes a second least significant bit ~~M[1]~~ and a sum ~~SPPI[1:0]~~ of the previous sum and current partial product.

8. (currently amended) The multiple modulus selector ~~as recited in~~ of claim 2, wherein the first selection signal includes two bits ~~SEL_MM[1:0]~~.

9. (currently amended) The multiple modulus selector ~~as recited in~~ of claim 2, wherein the modulus selector further generates a multiple modulus accumulation indicating signal ~~SEL_M2~~ that is input to an accumulator.

10. (currently amended) The multiple modulus selector ~~as recited in~~ of claim 2, wherein the multiplicand includes two bits ~~$SSPP_i[1:0]$~~.

11. (currently amended) The multiple modulus selector ~~as recited in~~ of claim 2, wherein the second selection signal includes two bits ~~SEL_M1[1:0]~~.

12. (currently amended) A Montgomery modular multiplier of a computer system, communication network, or computer system and communication network that uses a public-key cryptographic algorithm, the Montgomery modular multiplier comprising:

a multiple modulus selector ~~for selecting~~ adapted to select one of -M, 0, M, and 2M (M being an n-bit modulus number) as a multiple modulus in an integer modular multiplication mode, and ~~selecting~~ adapted to select one of 0, M, and 2M as a multiple modulus in a polynomial modular multiplication mode to output a multiple modulus accumulation indicating signal ~~SEL_M2~~;

a [[booth]] Booth recoder ~~for providing~~ adapted to provide a first value used to obtain a partial product value; and

an accumulator ~~for summing~~ adapted to sum second values to obtain a result of the Montgomery multiplier[[,]];

wherein the accumulator sums the modulus M and the second values based on the multiple modulus accumulation indicating signal ~~SEL_M2~~ in the polynomial modular multiplication mode.

13. (currently amended) The Montgomery multiplier ~~as recited in~~ of claim 12, further comprising:

a modulus number register ~~for storing~~ adapted to store a modulus value [[there]]in the modulus number register;

a multiplicand register ~~for storing~~ adapted to store a multiplicand value [[there]]in the multiplicand register;

a multiplicator register ~~for storing~~ adapted to store a multiplicator value [[there]]in the multiplicator register;

an AND gate ~~for combining~~ adapted to combine the multiplicator value with the multiplicand value; and

two adders ~~for combining~~ adapted to combine the values from the accumulator and the AND gate to output a combined value[[,]];

wherein the combined value is input to the multiple modulus selector.

14. (currently amended) The Montgomery multiplier ~~as recited in~~ of claim 12, wherein the multiple modulus selector comprises:

a modulus recoder ~~for receiving~~ adapted to receive an n-bit modulus M, a previous sum, and a current partial product to generate a first selection signal;

a modulus selector ~~for receiving~~ adapted to receive the n-bit modulus M, the previous sum, the current partial product, and a multiplicand to generate a second selection signal; and

a multiplexer ~~for receiving~~ adapted to receive inputs -M, 0, M, and 2M, ~~and selecting~~ adapted to select one of the inputs -M, 0, M, and 2M based on the first selection signal in an integer modular multiplication mode, and ~~selecting~~ adapted to select one of the inputs 0, M, and 2M based on the second selection signal in a polynomial modular multiplication mode.

15. (currently amended) The Montgomery multiplier ~~as recited in~~ of claim 12, wherein the [[booth]] Booth recoder comprises:

a first selector ~~for receiving~~ adapted to receive a multiplicator to generate a third selection signal ~~SEL_PP[1:0]~~;

a second selector ~~for receiving~~ adapted to receive the multiplicator to generate a fourth selection signal ~~SEL_A1[1:0]~~; and

a multiplexer ~~for receiving~~ adapted to receive inputs [[-]]~~M, 0, M, and 2M~~ -2A, -A, 0, A, 2A, ~~and selecting~~ adapted to select one of the inputs -2A, -A, 0, A, 2A based on the third selection signal in an integer modular multiplication mode, and ~~selecting~~ adapted to select one of the inputs 0, A, and

2A based on the fourth selection signal in a polynomial modular multiplication mode.

16. (currently amended) A modulus selector of a computer system, communication network, or computer system and communication network that uses a public-key cryptographic algorithm for receiving [[the]] an n-bit modulus M, [[the]] a previous sum, [[the]] a current partial product, and a multiplicand to generate a second selection signal, the modulus selector comprising:

a modulus selector unit ~~for receiving an~~ adapted to receive the n-bit modulus M, [[a]] the previous sum, [[a]] the current partial product, and [[a]] the multiplicand to generate [[a]] the second selection signal, ~~for selecting~~ and adapted to select one of the three values 0, M, and 2M, that is input to a multiplexer and a modulus accumulation indicating signal that is input to an accumulator.

17. (currently amended) A [[booth]] Booth recoder of a computer system, communication network, or computer system and communication network that uses a public-key cryptographic algorithm, the Booth recoder comprising:

a first selector ~~for receiving~~ adapted to receive a multiplicator to generate a first selection signal ~~SEL_PP[1:0]~~;

a second selector ~~for receiving~~ adapted to receive the multiplicator to generate a ~~seecond~~ second selection signal ~~SEL_A1[1:0]~~; and

a multiplexer ~~for receiving~~ adapted to receive first inputs [[-]]~~M, 0, M, and 2M~~ -2A, -A, 0, A, 2A, ~~and selecting~~ adapted to select one of the first inputs -2A, -A, 0, A, 2A based on the first selection signal in an integer modular multiplication mode, ~~and receiving~~ adapted to receive second inputs 0, A, and 2A, and ~~selecting~~ adapted to select one of the second inputs 0, A, and 2A based on the second selection signal in a polynomial modular multiplication mode.